WHAT IS CLAIMED IS:

1. A method of processing information in a communications device, comprising:

(a) receiving from a first remote device content encrypted with a content key;

(b) transmitting a request for the content key to a second remote device, the second remote device authorized to act on behalf of a provider of the content;

(c) receiving from the second remote device an encrypted version of the content key, wherein the encrypted version of the content key is encrypted with a public key of the communications device; and

(d) decrypting the encrypted version of the content key with a private key of the communications device, the private key of the communications device corresponding to the public key of the communications device.

2. The method of claim 1, wherein step (b) comprises transmitting the public key of the communications device to the second remote device.

3. The method of claim 1, further comprising:

receiving from the first remote device the content key encrypted with a public key of the second remote device.

4. The method of claim 3, wherein step (b) comprises transmitting to the second remote device the content key encrypted with the public key of the second remote device.

5. The method of claim 4, wherein step (b) further comprises transmitting to the second remote device the public key of the communications device.

6. The method of claim 1, further comprising:

receiving one or more usage rules from the first remote device, wherein the usage rules correspond to the content;

transmitting the one or more usage rules to the second remote device;

receiving one or more modified usage rules from the second remote device; and

associating the one or more modified usage rules with the content.

7. A communications device, comprising:

a first communications interface adapted to receive from a first remote device content encrypted with a content key;

a module adapted to decrypt an encrypted version of the content key with a private key of the communications device; and

a second communications interface adapted to

(a) transmit a request for the content key to a second remote device, the second remote device authorized to act on behalf of a provider of the content, and

(b) receive from the second remote device an encrypted version of the content key, wherein the encrypted version of the content key is encrypted with a public key of the communications device, the public key of the communications device corresponding to the private key of the communications device.

8. The device of claim 7, wherein the request includes the public key of the communications device.

9. The device of claim 7, wherein the first communications interface is further adapted to receive from the first remote device the content key encrypted with a public key of the second remote device.

10. The device of claim 9, wherein the request includes the content key encrypted with the public key of the second remote device.

11. The device of claim 10, wherein the request includes the public key of the communications device.

12. The device of claim 7, wherein the first communications interface is further adapted to receive one or more usage rules from the first remote device, the usage rules corresponding to the content; and

wherein the second communications interface is further adapted to transmit the one or more usage rules to the second remote device; and to receive one or more modified usage rules from the second remote device.

13. A communications device, comprising:

means for receiving from a first remote device content encrypted with a content key;

means for transmitting a request for the content key to a second remote device, the second remote device authorized to act on behalf of a provider of the content;

means for receiving from the second remote device an encrypted version of the content key, wherein the encrypted version of the content key is encrypted with a public key of the communications device; and

means for decrypting the encrypted version of the content key with a private key of the communications device, the private key of the communications device corresponding to the public key of the communications device.

14. A system, comprising:

a communications device adapted to receive from a remote device a content item encrypted with a content key; and

an authorized agent authorized to act on behalf of a content distributor, the authorized agent adapted to provide the content key to the communications device.

15. The system of claim 14, wherein the communications device is further adapted to transmit a request for the content key to the authorized agent.

16. The system of claim 15, wherein the request includes a public key of the communications device.

17. The system of claim 15, wherein the request includes the content key encrypted with a public key of the authorized agent.

18. The system of claim 14, wherein the authorized agent is further adapted to provide to the communications device the content key encrypted with a public key of the communications device.

19. The system of claim 14, further comprising the content distributor.

20. The system of claim 19, further comprising the remote device;
wherein the remote device receives the content item from the content distributor.

21. The system of claim 14, wherein the communications device, the remote device, and the authorized agent communicate with each other across one or more wireless communications networks.

22. A method of facilitating distribution of content among devices in an authorized agent, comprising:

(a) receiving authorization to act on behalf of a content distributor;

(b) receiving from a communications device a request for a content key, the content key for decrypting a content item originally distributed by the content distributor;

(c) encrypting the content key with a public key of the communications device; and

(d) transmitting to the communications device the content key encrypted with the public key of the communications device.

23. The method of claim 22, further comprising:

(e) receiving the content key encrypted with a public key of the authorized agent.

24. The method of claim 23, wherein step (e) comprises receiving the content key encrypted with the public key of the authorized agent from the communications device.

25. The method of claim 23, wherein step (e) comprises receiving the content key encrypted with the public key of the authorized agent from the content distributor.

26. The method of claim 23, wherein step (b) comprises receiving the public key of the communications device.

27. The method of claim 26, further comprising:

decrypting the content key encrypted with the public key of the authorized agent; and

encrypting the content key with the public key of the communications device.

28. The method of claim 22, further comprising:

receiving one or more usage rules from the communications device, the one or more usage rules corresponding to the content item;

modifying the one or more usage rules; and

transmitting the one or more modified usage rules to the communications device.

29. The method of claim 28, wherein said modifying step is performed in accordance with one or more modification limitations.

30. The method of claim 29, wherein the one or more modification limitations includes at least one of a temporal limitation, a content type limitation, and a specific content limitation.

31. The method of claim 29, wherein the one or more modification limitations are imposed by the content distributor.

32. The method of claim 28, wherein the one or more usage rules are encrypted with a public key of the authorized agent.

33. The method of claim 28, wherein the one or more modified usage rules are encrypted with a public key of the communications device.

34. The method of claim 22, wherein step (d) is performed when one or more content distribution conditions are satisfied.

35. The method of claim 34, wherein the one or more content distribution conditions includes a payment from the communications device.

36. An authorized agent, comprising:

a first communications interface adapted to receive authorization to act on behalf of the content distributor;

a module adapted to encrypt a content key with a public key of the communications device, the content key for decrypting a content item originally distributed by the content distributor; and

a second communications interface adapted to receive from a communications device a request for the content key, and transmit to the communications device the content key encrypted with the public key of the communications device.

37. The authorized agent of claim 36, wherein the request includes the content key encrypted with a public key of the authorized agent.

38. The authorized agent of claim 36, wherein the first communications interface is further adapted to receive the content key encrypted with a public key of the authorized agent from the content distributor.

39. The authorized agent of claim 37, wherein the request further includes the public key of the communications device.

40. The authorized agent of claim 39, further comprising a module adapted to decrypt the content key encrypted with the public key of the authorized agent.

41. The authorized agent of claim 36, further comprising a rules module adapted to modify one or more usage rules received from the communications device; and

wherein the second communications interface is further adapted to send the one or more modified rules to the communications device.

42. The authorized agent of claim 41, wherein said rules module is further adapted to modify the one or more usage rules in accordance with one or more modification limitations.

43. The authorized agent of claim 42, wherein the one or more modification limitations includes at least one of a temporal limitation, a content type limitation, and a specific content limitation.

44. The authorized agent of claim 42, wherein the one or more modification limitations are imposed by the content distributor.

45. The authorized agent of claim 41, wherein the one or more usage rules are encrypted with a public key of the authorized agent

46. The authorized agent of claim 41, wherein the one or more modified usage rules are encrypted with a public key of the communications device.

47. The authorized agent of claim 36, wherein said second communications interface is further adapted to transmit the content key encrypted with the public key of the communications device when one or more content distribution conditions are satisfied.

48. The authorized agent of claim 47, wherein the one or more content distribution conditions includes a payment from the communications device.

49. A system, comprising:

means for receiving authorization to act on behalf of a content distributor;

means for receiving from a communications device a request for a content key, the content key for decrypting a content item originally distributed by the content distributor;

means for encrypting the content key with a public key of the communications device; and

means for transmitting to the communications device the content key encrypted with the public key of the communications device.

50. A system, comprising:

a content distributor adapted to transmit a digital television broadcast along with a public encryption key of an authorized agent, the authorized agent authorized to act on behalf of the content distributor; and

a communications device adapted to receive the digital television broadcast and the public encryption key from the content distributor;

wherein the communications device is further adapted to encrypt the digital television broadcast with an internally generated content key, and to encrypt the internally generated content key with the public key of the authorized agent.

51. A communications device, comprising:

a communications interface adapted to receive from a content distributor a digital television broadcast and a public encryption key of an authorized agent, the authorized agent authorized to act on behalf of the content distributor; and

a security processing module adapted to encrypt the digital television broadcast with an internally generated content key, and to encrypt the internally generated content key with the public key of the authorized agent.